PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) **International Patent Classification** 7 :
E05B 49/00, G08C 19/28

A1

(11) **International Publication Number:** **WO 00/12850**

(43) **International Publication Date:** 9 March 2000 (09.03.00)

(21) **International Application Number:** PCT/US99/19680

(22) **International Filing Date:** 26 August 1999 (26.08.99)

(30) **Priority Data:**
09/140,022 26 August 1998 (26.08.98) US

(71) **Applicant:** LEAR CORPORATION [US/US]; 21557 Telegraph Road, Southfield, MI 48034 (US).

(72) **Inventor:** KING, Joseph, D.; 3634 Patridge Path #7, Ann Arbor, MI 48108 (US).

(74) **Agents:** HALLER, Timothy, J. et al.; Niro, Scavone, Haller & Niro, Suite 4600, 181 W. Madison, Chicago, IL 60602 (US).

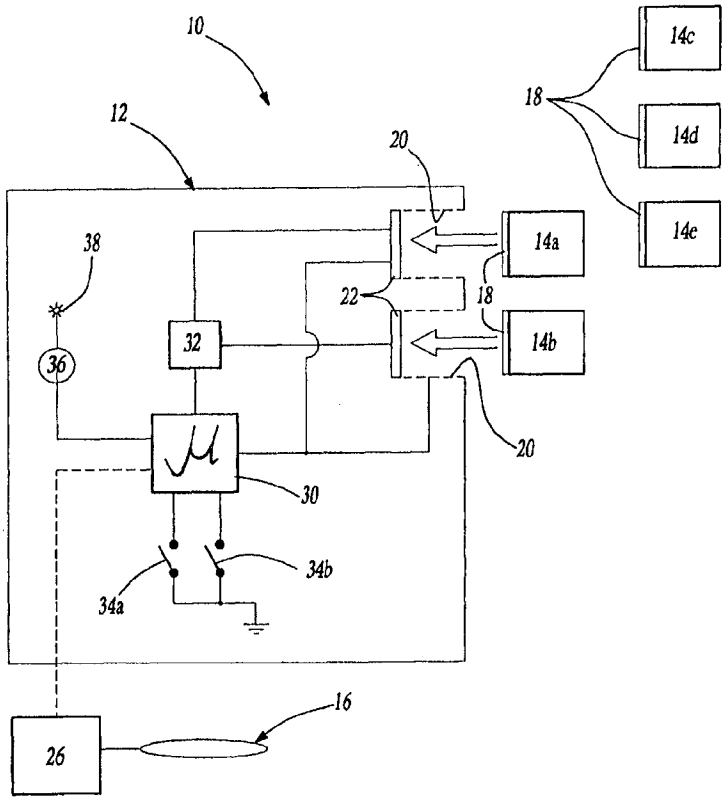
(81) **Designated States:** JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) **Title:** RECONFIGURABLE UNIVERSAL TRAINABLE TRANSMITTER

(57) **Abstract**

A trainable transmitter (12) comprises a transmitter, code–generation circuitry (30) and a removable, plug–in data module (14a–14e, 16). The data module includes information necessary for generating a code for a specific security system, such as a garage door opener. Preferably, the data includes a cryptographic algorithm and the frequency at which the wireless signal is to be generated. The code–generation circuitry accesses the data in the data module to generate a code, which is then transmitted by the transmitter. A variety of data modules are provided. A user installs a data module which corresponds to the security system to be accessed.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

RECONFIGURABLE UNIVERSAL TRAINABLE TRANSMITTER

BACKGROUND ART

The present invention relates generally to wireless trainable transmitters, particularly for vehicles.

Increasing numbers of new vehicles are being sold with trainable transmitters permanently installed in the vehicle. The trainable transmitters allow consumers to train the transmitter to duplicate an existing transmitter, such as a garage door opener. This approach provides certain advantages. For example, since the transmitter is permanently installed, it is more difficult for a thief to steal the transmitter while obtaining the owner's address from the glove compartment. Further, the current trainable transmitters pre-store a plurality of cryptographic algorithms allowing the trainable transmitter to be universal. This provides convenience to the consumer by allowing the trainable transmitter to be compatible with many home products, such as garage door openers.

However, a permanently installed trainable transmitter that pre-stores a plurality of cryptographic algorithms suffers from some disadvantages. The universal trainable transmitter, by virtue of its learning capability and pre-storing a plurality of cryptographic algorithms, is simply a universal code grabber. A person with basic electrical/electronic knowledge can increase the range with commercially available RF amplifiers to convert the trainable transmitter to a code grabber. A potential thief could construct such a code grabber and steal codes from a victim's garage door opener transmitter. Since the universal trainable transmitter pre-stores a plurality of cryptographic algorithms, even advanced rolling codes could be compromised.

Further, current universal trainable transmitters cannot be upgraded to new cryptographic algorithms as the manufacturers of home products (*e.g.*, garage doors, home security entry systems, and wireless switches) change existing codes. Additionally, a universal trainable transmitter would not be compatible with new wireless products by new manufacturers, since there is no common standard for rolling security codes. Since different manufacturers use different codes and encryption algorithms, the universal trainable transmitter cannot be 100% universal or upgradable.

DISCLOSURE OF INVENTION

The present invention provides a re-configurable trainable transmitter including a removable plug-in data module which contains a cryptographic algorithm and the other information necessary for generating a wireless signal containing a code associated with a specific security system. The trainable transmitter generally comprises a transmitter and code-generation circuitry, such as a microprocessor. The microprocessor generates a digital code based upon the data in the data module, including the cryptographic algorithm. The microprocessor determines a digital code based upon the cryptographic algorithm and the transmitter generates a wireless signal including the digital code at a frequency also specified by the data module.

Preferably, the data module is associated with a security system from a certain manufacturer or of a specified model or models. Initially, a user would obtain the correct data module necessary to operate the user's security system, such as garage door opener or home security system, either from the manufacturer of the security system or the manufacturer of the vehicle. By providing the correct plug-in data module, no learning mode would be required. Further, it would not be necessary to store the cryptographic algorithms from the many manufacturers on the trainable transmitter. Only the cryptographic algorithm to be used would be stored on the trainable transmitter.

BRIEF DESCRIPTION OF THE DRAWINGS

The above, as well as other advantages of the present invention, will become readily apparent to those skilled in the art from the following detailed description of a preferred embodiment when considered in the light of the accompanying drawings in which:

Figure 1 is a schematic of the trainable transmitter of the present invention; and

Figure 2 illustrates the trainable transmitter installed in a vehicle.

BEST MODE OF CARRYING OUT THE INVENTION

A vehicle transmitter system 10 is shown in Figure 1 generally comprising a reconfigurable trainable transmitter 12 at a plurality of data modules 14a-e and 16. Preferably, the data modules 14 are each ROM chips having electrical connectors 18 such as connector pins or other known electrical connectors. The data modules 14 are each stored in a cartridge which can be handled by consumers. The data module 16 is preferably a CD ROM 16.

The data modules 14a-e each contain different data necessary to generate a digital code for a different security system. For example, each data module 14a-e contains a cryptographic algorithm for generating a rolling code and an indication of the frequency at which the wireless signal containing the digital code is to be generated. The data module 14 may also include other information regarding the modulation protocol of the wireless signal to be sent. Again, each of the data modules 14a-e contains only sufficient information for a single security system. Some of the data modules 14a-e may simply contain a single digital code, for security systems which do not use encrypted codes. Each of the data modules 14 is associated with a specific model or models from specific manufacturers of security systems, such as garage door openers.

The trainable transmitter 12 includes at least one, but alternatively more than one, socket 20 to which the data modules 14 can be connected. The socket 20 includes electrical connectors 22 which electrically connect to the electrical connector 18 on the data modules 14.

The CD ROM 16 stores "personality" information for a plurality of security systems, including cryptographic algorithms, frequencies, modulation schemes, etc. The CD ROM 16 is readable by a CD player 26 which is installed in a location remote from the trainable transmitter 12, but electrically connected to the trainable transmitter 12. The trainable transmitter 12 includes code-generation circuitry 30, preferably a microprocessor executing appropriate software. The code-generation circuitry 30 could alternatively comprise hard-wired circuitry. Tamper detection circuitry 32 is connected to the sockets 20 and the code-generation circuitry 30.

The code-generation circuitry 30 receives inputs from user-activated switches 34a and 34b. The code-generation circuitry generates a digital code and sends it to an oscillator 36, which is preferably a voltage-controlled oscillator or other variable frequency oscillator, or a plurality of discrete oscillators, such that more than one frequency can be generated. The oscillator transmits a wireless signal, preferably RF, via an antenna 38.

Figure 2 illustrates the vehicle transmitter system 10 installed in a vehicle 40. Preferably, the trainable transmitter 12 is installed in a headliner 42 of the vehicle 40. If the optional CD ROM player 26 with the CD ROM 16 is utilized, the CD player 26 and CD ROM 16 is preferably installed in the vehicle 40 at a location remote from the trainable transmitter 12 and connected via wires, or other means.

In operation, a user initially selects one of the data modules 14a-e which corresponds to the garage door opener (or other security system) that the user wishes the vehicle transmitter system 10 to operate. The selected data module 14 must have the same cryptographic algorithm, frequency, modulation, etc. that the receiving garage door opener receiver utilizes.

The trainable transmitter 12 is placed in a "train" mode, using user input switches 34a-b (or others) along with the security systems 44a-b. In the train mode, the trainable transmitter 12 is synchronized with the systems 44a-b with respect to the cryptographic algorithms. It should be noted that this is different than a "learn" mode where the cryptographic algorithm, frequency or modulation is learned from other systems. This data which is learned from other systems is supplied by the data modules 14.

In operation, referring to Figures 1 and 2, when the user activates one of the switches 34a, for example, the code-generation circuitry 30 accesses the corresponding data module 14a to obtain the code-generation algorithms and other data. The code-generation circuitry 30 then generates the appropriate digital code, which is transmitted via the antenna 38 by the oscillator 36. This wireless signal is received by the receiving system 44a, such as a garage door opener. Upon receiving the digital code, the receiving system 44a activates the system, such as opening or closing the garage

door. When the user activates the second switch 34b, the code-generation circuitry 30 accesses the second data module 14b and generates a second digital code, based upon a second cryptographic algorithm. This second digital code is transmitted via the antenna 38 by the oscillator 36, possibly at a second frequency and utilizing a second modulation scheme. This wireless signal is received by the second receiving system 44b, such as a home security system, which activates the system based upon receiving the proper digital code.

The tamper detection circuitry 32 is connected to the code-generation circuitry 30 and indicates to the code-generation circuitry 30 when the trainable transmitter 12 is removed from the vehicle 40. The tamper detection circuitry 32 may simply monitor power to the trainable transmitter 12, or include an interlock connection to the vehicle such as an electrical connection to the vehicle body which when broken indicates that the trainable transmitter 12 is removed from the vehicle. Alternatively, the tamper detection circuitry can include an LED which reflects light from a surface on the vehicle 40; when the trainable transmitter 12 is removed from the vehicle 40, the light is no longer reflected from the LED off of the vehicle surface, thereby indicating that the trainable transmitter 12 has been removed.

When the tamper detection circuitry 32 detects that the trainable transmitter 12 has been removed from the vehicle 40, the trainable transmitter 12 is rendered permanently unusable in one of several ways. First, the tamper detection circuitry 32 (or the code-generation circuitry 30) can erase the data from the data modules 14a-b (which may be EEPROM). Alternatively, the tamper detection circuitry 32 can erase the memory in or otherwise disable the code-generation circuitry 30. In this manner, if the trainable transmitter 12 is permanently installed in the vehicle 40, unauthorized removal and use can be prevented. Of course, the tamper detection circuitry 32 would not be utilized if the trainable transmitter 12 is a portable transmitter, such as a fob.

In the alternate embodiment, utilizing the CD ROM 16, the code-generation circuitry 30 accesses the data on the CD ROM 16, when necessary to generate a digital code, *i.e.*, upon activation of one of the user-activated switches 34a-b. In this embodiment, the code-generation circuitry 30 can utilize a learn mode to learn the

algorithm, frequency, modulation, etc., which is then accessed from the CD ROM 16. Alternatively, the specific make and model of the security system can be indicated to the trainable transmitter 12 or CD player 26 so that the proper data is transmitted from the CD ROM 16 to the code-generation circuitry 30. In this embodiment, if the trainable transmitter 12 is ever removed from the vehicle, the data for the plurality of security systems would remain in the vehicle 40. Thus, the stolen trainable transmitter 12 would not constitute the universal code grabber. Nor would the trainable transmitter 12 be able to activate the security systems 44a&b without the data.

The trainable transmitter 12 of the present invention provides a universal trainable transmitter 12 that does not have the capability of being transformed into a universal code grabber. However, the trainable transmitter 12 can be utilized with many different security systems from different manufacturers, in conjunction with the data modules 14 and/or 16.

CLAIMS

1. A trainable transmitter comprising:

a transmitter for transmitting a code in a wireless signal; and

a data module connectable to said transmitter, said data module including data necessary to generate said code.

2. The trainable transmitter of Claim 1, wherein said data includes a cryptographic algorithm.

3. The trainable transmitter of Claim 1, wherein said data includes a frequency at which the wireless signal should be transmitted.

4. The trainable transmitter of Claim 1, wherein said data module is ROM.

5. The trainable transmitter of Claim 1, wherein said data module is removably secured to said trainable transmitter and removably connected to said transmitter.

6. The trainable transmitter of Claim 1 further including code-generation circuitry, said code-generation circuitry generating said code to be transmitted by said transmitter based upon said data in said data module.

7. The trainable transmitter of Claim 1, wherein said data module is mounted remotely from said transmitter.

8. The trainable transmitter of Claim 1, wherein said transmitter is mounted in a vehicle.

9. The trainable transmitter of Claim 8, wherein said data module is installed in a remote location in the vehicle from the transmitter.

10. The trainable transmitter of Claim 1, wherein said data module includes a plurality of cryptographic algorithms.

11. The trainable transmitter of Claim 1, wherein said data module includes said data for a plurality of wireless communication systems.

12. The trainable transmitter of Claim 1, further including tamper detection circuitry, said trainable transmitter disabling said code-generation circuitry based upon detection of tampering with said trainable transmitter by said tamper detection circuitry.

13. A data module for a trainable transmitter comprising:

a computer storage media storing data necessary for generating a code for a security system.

14. The data module of Claim 13, wherein said data includes a cryptographic algorithm.

15. The data module of Claim 14, wherein said data includes a frequency at which a wireless signal is to be transmitted.

16. The data module of Claim 15, wherein said storage media is ROM.

17. The data module of Claim 16 further including a connector for providing electrical connection to a transmitter.

18. The data module of Claim 13, wherein said data includes a plurality of cryptographic algorithms.

19. A trainable transmitter comprising:

a ROM data module connectable to said transmitter, said data module including a cryptographic algorithm;

a transmitter for transmitting a wireless signal; and

code-generation circuitry, said code-generation circuitry generating said code to be transmitted by said transmitter based upon said data in said data module, said data module removable secured to said code-generation circuitry.

20. The trainable transmitter of Claim __ further comprising:

a plurality of said ROM data modules, each including a different cryptographic algorithm.

21. A method for generating a wireless signal including the steps of:

a) selecting a data module containing a cryptographic algorithm for generating a digital code for a security system from among a plurality of data modules each having different cryptographic algorithm;

b) connecting the data module selected in said step a) to code-generation circuitry;

c) generating a digital code based upon the cryptographic algorithm in the selected data module in the code-generation circuitry; and

d) transmitting the digital code in a wireless signal.

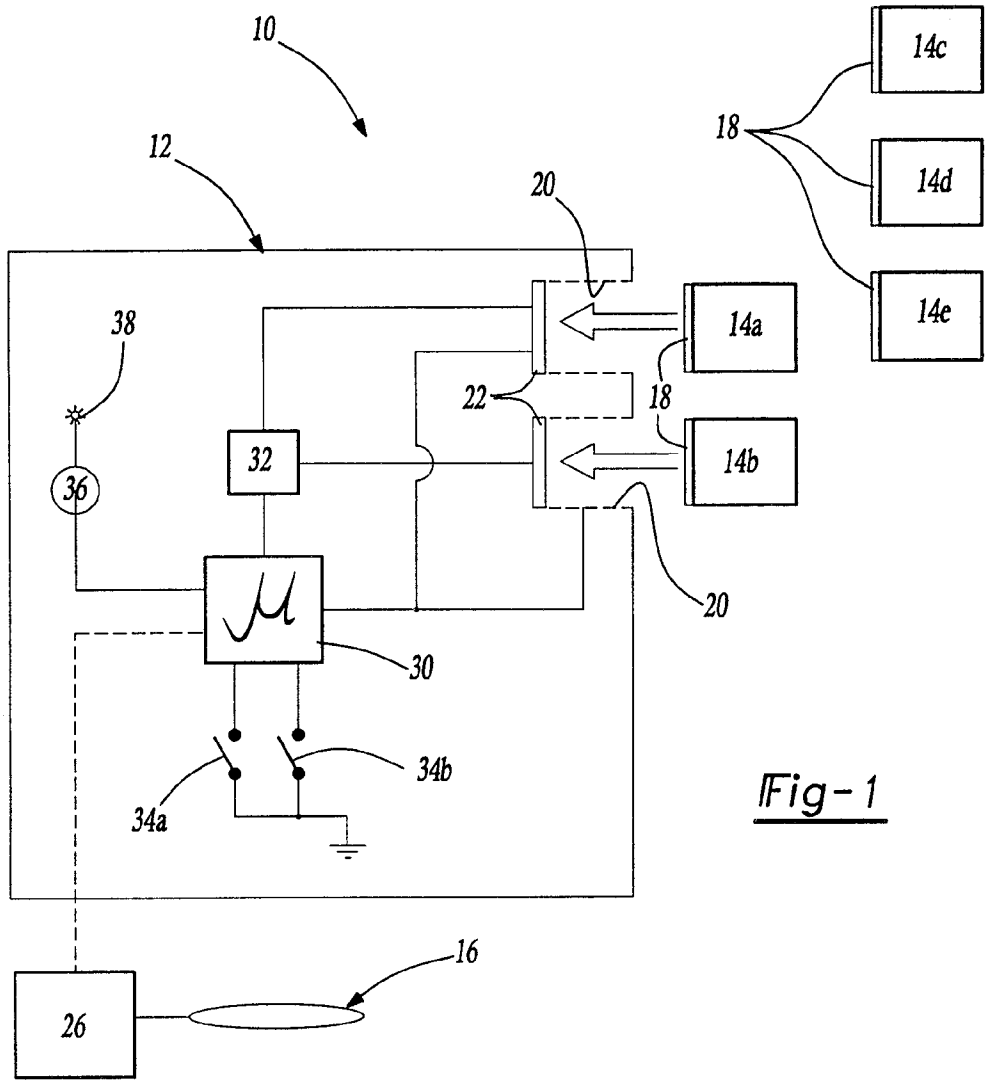

10
12
14c
18
14d
14e
20
14a
38
22
18
14b
32
36
20
30
34b
34a
16
26

Fig-1

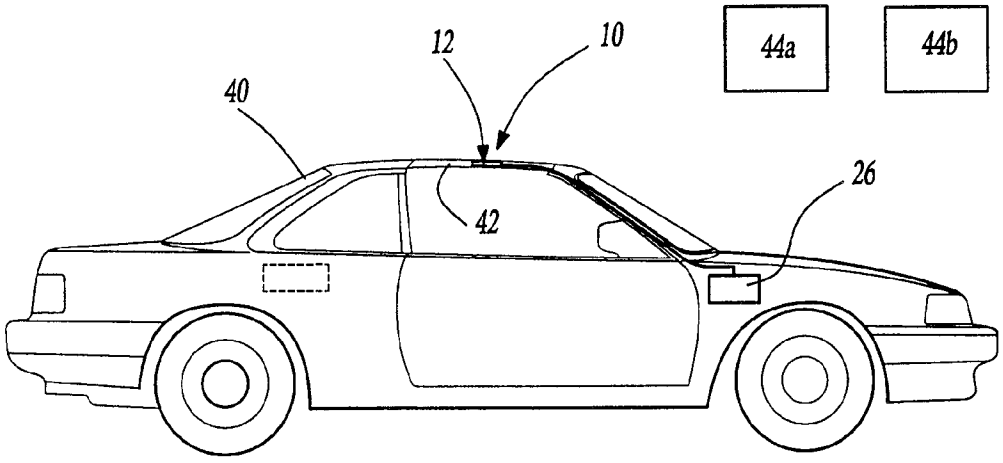

44a
44b
12
10
40
26
42

Fig-2

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/US 99/19680

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00 G08C19/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B G08C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Adaptable remote control device" RESEARCH DISCLOSURE., no. 352, 1 August 1993 (1993-08-01), page 552 XP000395279 INDUSTRIAL OPPORTUNITIES LTD. HAVANT., GB ISSN: 0374-4353	1,5,17
A	figures 1,2	6,11,19, 20

X	DE 196 44 237 A (LINDMAYER,BOOM) 30 April 1998 (1998-04-30)	1,5,6
A	column 2, line 13 -column 3, line 15; figure 1	11,17,19

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 1999	22/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herbelet, J.C.

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 99/19680

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 608 758 A (SUSUMU SAKUMA AND OTHERS) 4 March 1997 (1997-03-04) column 9, line 34 -column 12, line 64; figures 1-3	1,3-6, 15-17, 19,20
A	FR 2 650 420 A (CARDINI) 1 February 1991 (1991-02-01)	
A	GB 2 287 337 A (PRINCE CORPORATION) 13 September 1995 (1995-09-13)	

1

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/US 99/19680

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19644237 A	30-04-1998	NONE	
US 5608758 A	04-03-1997	DE 4323795 A	20-01-1994
		GB 2270218 A,B	02-03-1994
		GB 2301962 A,B	18-12-1996
		GB 2301963 A,B	18-12-1996
		US 5764697 A	09-06-1998
FR 2650420 A	01-02-1991	IT 218519 Z	27-05-1992
		GB 2246890 A	12-02-1992
GB 2287337 A	13-09-1995	US 5627529 A	06-05-1997
		DE 19508276 A	14-09-1995
		GB 2297411 A,B	31-07-1996
		GB 2297412 A,B	31-07-1996
		GB 2297413 A,B	31-07-1996
		JP 7290952 A	07-11-1995
		US 5646701 A	08-07-1997
		US 5619190 A	08-04-1997